

00/8119
ISR 3/18/9

(19)



JAPANESE PATENT OFFICE

(5)

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000029792 A

(43) Date of publication of application: 28 . 01 . 00

(51) Int. Cl

G06F 12/14

(21) Application number: 10195353

(71) Applicant: HITACHI LTD

(22) Date of filing: 10 . 07 . 98

(72) Inventor: TOMIZAWA SATOSHI

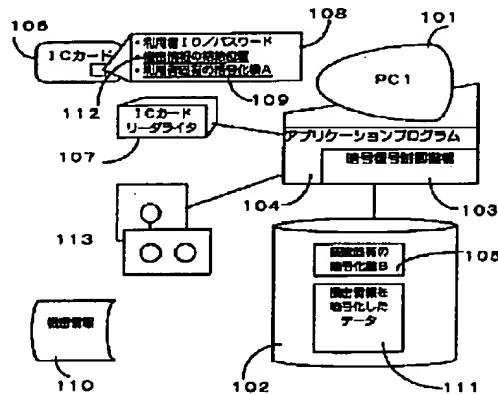
(54) SECRET INFORMATION STORAGE DEVICE

COPYRIGHT: (C)2000,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To improve the confidentiality by storing information on a user, information showing the storage destination of secret information, and an encoding key characteristic of the user on a small-capacity medium and generating and storing a key characteristic of the device on a hard disk.

SOLUTION: At incorporating, a key B105 characteristic of the device is generated and stored on an external storage device 102. Then the user actuates an encoding control mechanism 103 to register information 108 on the user. The contents of the information 108 of the user consist of a user ID, a password, and the encoding key A109 characteristic of the user. Then the user specifies desired secret information 110 to be concealed. An encoding control mechanism 103 reads the secret information 110 out and encodes it with a key A109 characteristic of the user. Consequently, a file obtained by further encoding the obtained file with the encoding key 105 characteristic of the device is written to a location such that the user specifies on the external storage device of the device. The location that the user specifies is written as a storage location 112 of the confidential information to an IC card 106.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-29792
(P2000-29792A)

(43)公開日 平成12年1月28日(2000.1.28)

(51)Int.Cl.⁷
G 0 6 F 12/14

識別記号
3 2 0

F I
G 0 6 F 12/14

テーマコード(参考)
3 2 0 C 5 B 0 1 7

審査請求 未請求 請求項の数 3 OL (全 8 頁)

(21)出願番号 特願平10-195353

(22)出願日 平成10年7月10日(1998.7.10)

(71)出願人 000005108

株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地

(72)発明者 富澤 智
神奈川県川崎市幸区鹿島田890番地 株式
会社日立製作所情報システム事業部内

(74)代理人 100068504
弁理士 小川 勝男

Fターム(参考) 5B017 AA06 BA05 BA07 CA14

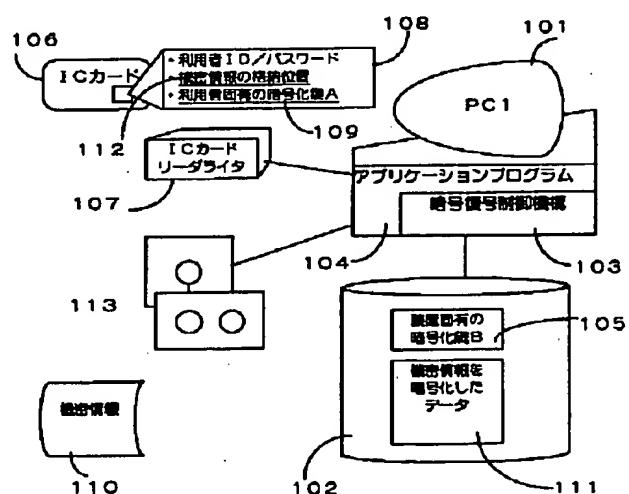
(54)【発明の名称】 機密情報格納装置

(57)【要約】

【課題】格納された利用者の情報と利用者の入力情報を突き合わせて正しい時、機密情報にアクセスするための鍵を取出す方法などでは、利用者の情報と機密情報または機密情報にアクセスする鍵が同一の媒体に格納され意の第三者により媒体自身が盗まれた場合、総当たり的な方法で利用者の機密情報または機密情報にアクセスするための鍵を取出すことができる危険性がある。

【解決手段】本発明では機密情報を格納する時に利用者固有の鍵と装置固有の鍵とを使用することにより、暗号化し、より機密性の高い情報の格納方法を提供するものである。

図1



【特許請求の範囲】

【請求項1】装置固有の鍵を生成し保管する手段と、利用者の認証が正常に行われた時のみ小容量媒体に格納された鍵と、装置固有の鍵を取り出す手段と、それらの鍵を用いて機密情報を2重に暗号化し外部記憶装置に格納する手段と、これらの手段を制御する機構を備えることにより機密性を高めることを特徴とする機密情報格納装置。

【請求項2】装置固有の鍵を生成し保管する手段と、利用者の認証が正常に行われた時のみ小容量媒体に格納された鍵と、装置固有の鍵を取り出す手段と、それらの鍵を用いて2重に暗号化された外部記憶装置にある機密情報を復号する手段と、これらの手段を制御する機構を備えることにより機密性を高めることを特徴とする機密情報格納装置。

【請求項3】上記に加え、小容量媒体を用いた利用者の認証が正常に行われた時のみ装置固有の鍵を取り出し復号する手段と、装置固有の鍵で複合した機密情報（利用者の鍵で暗号化した機密情報）を媒体に書き込む手段と、利用者の認証が正常に行われた時のみ装置固有の鍵を取り出し媒体に書き込まれた利用者の鍵で暗号化された機密情報（装置固有の鍵で複合した機密情報）を装置固有の鍵で暗号化し外部記憶装置に格納する手段を備えることにより機密情報を不用意に複写されることを防ぐことを特徴とする請求項1又は2記載の機密情報格納装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンピュータの機密情報を保管する方法に関し、特に機密情報を格納する為の比較的容量の少ない携帯性に優れた媒体（ICカードなど）と比較的容量の大きい媒体（ハードディスクなど）を用いることにより機密情報を安全に格納・保管する方法に関する。

【0002】

【従来の技術】従来の方法ではICカードあるいはフロッピーディスク等の比較的容量の少ない運搬可能な媒体にユーザ情報（ユーザID、パスワードなど）を格納し、利用者により入力された利用者情報と突き合わせチェックを行うことにより、当該媒体に格納された機密情報にアクセス可能とすることで機密情報のアクセスを制限していた。あるいは同様の方法により当該媒体に格納された暗号鍵を取り出し機密情報を復号することにより機密情報へのアクセスを可能としている。

【0003】また別の方法としては利用者情報の一部（パスワードなど）をネットワークで接続された別のコンピュータに持たせることにより利用者情報の全部が盗まれることを回避しているが、インターネットのようなオープンなネットワーク上では通信中に悪意の第3者に盗聴される危険性を回避できないため盗聴されない為に

暗号化技術などを用いる必要がある。

【0004】

【発明が解決しようとする課題】かかる従来の方法においては次のような課題がある。すなわち①従来の方法では利用者情報と機密情報を同一の媒体に格納するため悪意を持った第3者に媒体ごと盗まれる危険性を考慮されておらず、その場合総当たり的な方法により機密情報あるいは機密情報にアクセスする為の鍵が盗まれてしまう。②利用者情報の一部（パスワードなど）をネットワークで接続された別のコンピュータに持たせることにより利用者情報の全部が盗まれることを回避する方法ではインターネットのようなオープンなネットワーク上では通信中に悪意の第3者に盗聴される危険性を回避できない。また盗聴されない為に通信プロトコル上の暗号化技術などを用いる必要がある。

【0005】

【課題を解決するための手段】本発明は、比較的容量の小さい運搬の容易な媒体A（例：ICカード、フロッピーディスク）に利用者の情報（利用者ID、パスワード）及び機密情報の格納先を示す情報、利用者固有の暗号化鍵Aを格納し、ハードディスク内に装置固有の鍵を生成して保有することにより、利用者が保管している媒体Aと利用者により入力される情報とハードディスク内のマシン固有の鍵とハードディスク内の暗号化された機密情報の全てが正当であった場合のみ機密情報をアクセス（閲覧、利用、変更）可能とする。

【0006】まず当該装置に対して利用者（もしくはブレインストールの場合、出荷元のメーカー）がソフトウェアを組み込む手順の中で装置固有の暗号化鍵Bを作成しハードディスクに保管する。装置固有の鍵の作り方は組み込まれた日付時刻やハードウェア固有のアドレス情報、あるいは乱数を用いて他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【0007】次に利用者の情報を登録する手順の中で利用者固有の鍵Aを作成し利用者情報とともに、携帯性の優れた媒体Aに格納する。利用者固有の鍵の作り方は利用者が登録された時刻や利用者の情報の一部（パスワード）、あるいは乱数を用いて他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【0008】これらの2つの鍵を用いて機密情報は二重に暗号化して保管される。暗号化の手順としては利用者固有の鍵Aによる暗号化、装置固有の鍵Bによる暗号化の順に行う。この理由は、利用者の鍵のみで暗号化した場合はハードディスク内の機密情報のファイルを複写し、当該装置に組み込まれたソフトウェアと同様のソフトウェアが組み込まれた別の装置において、総当たり的な方法により機密情報へのアクセスが可能になることを考慮している。

【0009】また、ハードディスクの故障を考慮した場合、機密情報を別の媒体に複写する必要があるが、媒体

Aを用い利用者情報が正しく入力された時のみ、鍵Bの復号化処理を行った出力ファイルを複写先の媒体に格納する機能を持たせる。複写先の媒体から別の装置のハードディスクに格納するには、媒体Aを用いて利用者登録した後、媒体Aと利用者の正当な入力があった時、初めて装置固有の鍵で暗号化してハードディスクに格納する機能により実現する。

【0010】

【発明の実施の形態】以下本発明実施の具体的方法を示す。

【0011】図1は本発明を適用する装置とその構成を示している。以下では携帯性に優れた比較的容量の小さい媒体をICカード、装置本体に固定的に接続される外部記憶装置をハードディスクとして記述する。本発明において、暗号化制御機構103はコンピュータ装置101の外部記憶装置102にアプリケーションプログラム104に含まれて組み込まれる。例えばアプリケーションプログラムは電子証明書を必要とする電子商取引のクライアントなどが考えられ、機密情報は電子証明書などが想定できる。

【0012】組み込みの際には、装置固有の鍵B105を作成し外部記憶装置102に格納する。装置固有の鍵B105の作り方は組み込まれた日付時刻やハードウェア固有のアドレス情報、あるいは乱数を用いて、他の装置と同一になる可能性が十分に小さいと判断できる方法で行う。

【0013】次に利用者が暗号化制御機構103を起動し利用者の情報を登録する。このとき暗号化制御機構103はICカードリーダライタ107により、初期化されたICカード106内に利用者の情報108を書き込む。利用者の情報108の内容は利用者ID/パスワード、利用者固有の暗号化鍵A109である。次に利用者が隠蔽しようとする機密情報110を指定する。

【0014】これは多くの場合外部媒体112により読み込まれる。暗号化制御機構103は機密情報110を読み取り利用者固有の鍵A109により暗号化する。この結果、得られたファイルを更に装置固有の暗号鍵105により暗号化した結果得られたファイルを装置の外部記憶装置内の利用者が指定した位置に書き込む。利用者が指定した位置はICカードの中に機密情報の格納位置112として書き込まれる。

【0015】以下、それぞれの処理の詳細を説明する。図2にアプリケーションプログラム104のインストール処理のフローを示す。プログラムのインストールを開始すると通常のインストールと同様にプログラムの組込み201を行う。201には必要なディレクトリの作成、必要なプログラムファイル等の圧縮解凍および複写、プログラム動作用環境変数の設定、レジストリの設定等が含まれる。

【0016】201が終了した後、装置固有の暗号鍵B

の生成202、鍵Bのハードディスクへの格納203を行いインストール処理を終了する。図3は利用者登録処理の流れを示している。まず利用者情報の読み込み(利用者ID)301、利用者情報の読み込み(パスワード)302を行う。これらは利用者による画面入力を読み取る方法で実施する。

【0017】次にICカードを読み取り303、データが既に存在する場合は初期化してよいかどうかを利用者に判断させる(304, 307)。その後利用者固有の暗号鍵Aを生成305し、利用者情報、暗号化鍵AをICカードに書き込む。図4は機密情報の格納処理1を示す。機密情報格納処理1は全く機密情報が暗号化されていない状態から暗号化されハードディスクに格納されるまでの処理である。

【0018】まず利用者情報、ICカードの読み込み(401, 402)利用者の入力が正しいかを判定し403、正しければ機密情報の読み込み404、ICカードから暗号化鍵Aを取り出し405、暗号化鍵Aで機密情報を暗号化406する。

【0019】次にハードディスクから装置固有の暗号化鍵Bを取り出し、鍵Aで暗号化された機密情報をさらに暗号化鍵Bで暗号化408する。最後に暗号化された機密情報の格納位置を利用者に問合わせ409、指定された格納位置情報をICカードに書き込む410とともに暗号化した機密情報を指定された格納位置に格納411する。なお、利用者情報の入力が正しくなく規定回数を超えた誤入力があった場合は処理を中止する(412, 413)。

【0020】図5、図6は上記で格納された暗号化された機密情報を別の媒体に複写する処理の手順と同様の機能がインストールされた別の装置のハードディスクに媒体を経由して機密情報を格納する方法を示す。図5の複写処理では、まず利用者情報の読み込み501、ICカードの読み込み502を行い入力が正しかった場合503は、ICカードから格納位置情報を読み取り504、格納位置に格納された暗号化された機密情報を読み込み505、暗号化鍵Bを取り出し506、機密情報の暗号化鍵Bによる複号化507を行う。次に複写先の位置を利用者から画面入力させ508、鍵Bで複合された機密情報(鍵Aで暗号化されている)を複写先に指定された媒体に格納509する。利用者情報の入力誤りは図4と同様(510, 511)。

【0021】図6の機密情報格納処理2(別の装置への格納処理)では、まず利用者情報の読み込み601、ICカードの読み込み602、利用者の入力が正しかった場合603には、入力元ファイルの位置情報を利用者に入力させ604、暗号化鍵Bで複号化された機密情報(暗号化鍵Aで暗号化されている)を入力元ファイルの位置から読み込み605、暗号化鍵B'を取り出し606(鍵B'：別の装置であるため鍵Bと異なることを意味す

る)、鍵B'により暗号化607する。

【0022】次に格納先の位置を利用者に入力させ608、暗号化した機密情報を指定された格納先に格納する609とともにICカード内の機密情報の格納位置情報を書き換える610。利用者情報の入力の誤りは図4の説明と同様である(611, 612)。

【0023】

【発明の効果】以上述べたように、本発明によれば装置内に格納された利用者の機密情報をICカードなどの運搬の容易な媒体と正当な利用者による入力が揃わなければ取り出すことができないよう保護することができ、また装置の故障にそなえ利用者が機密情報を別の媒体に簡単に複写できながら他の不正利用者による機密情報の複写を防止できる手段を提供できる。

【図面の簡単な説明】

【図1】本発明の機密情報格納装置の動作する装置の形態図。

【図2】本発明のソフトウェアのインストール処理の具体的なフローチャート図。

【図3】本発明のソフトウェアにおける利用者登録処理の具体的なフローチャート図。

【図4】本発明の機密情報格納処理1の具体的なフローチャート図。

【図5】本発明の機密情報複写処理の具体的なフローチャート図。

【図6】本発明の機密情報格納処理2の具体的なフローチャート図。

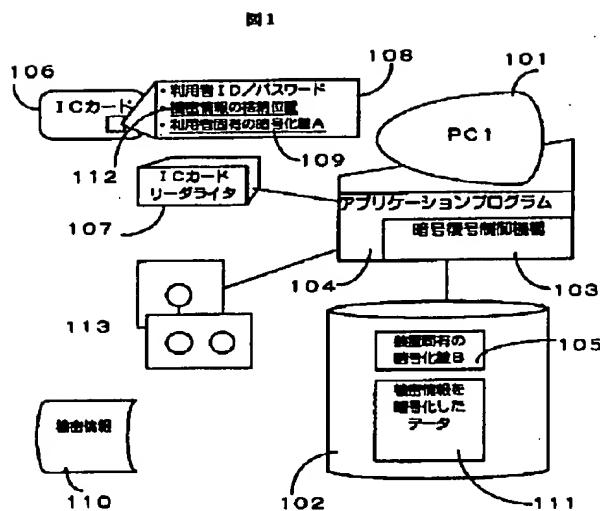
【符号の説明】

101…本発明のソフトウェアが動作するコンピュータ装置、102…装置に接続された外部記憶装置、103…本発明の機能となる暗号復号制御機構、104…暗号復号制御機構を含むアプリケーションプログラム、105…装置固有の暗号化鍵B、106…利用者の情報などを格納するICカード、107…ICカードリーダライタ、108…ICカードに格納された利用者固有の情報、109…利用者固有の暗号化鍵A、110…隠蔽したい機密情報、111…暗号化され格納された機密情報、112…機密情報の格納位置情報、113…入出力媒体(FD、DATなど)、200…プログラムインストール処理開始、201…プログラムの組込み、202…装置固有の鍵Bの生成処理、203…鍵Bのハ

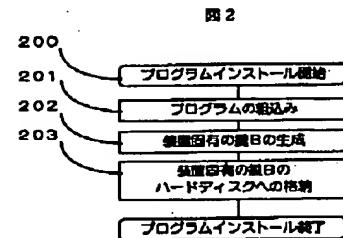
ードディスクへの格納、300…利用者登録処理開始、301…利用者情報の読み込み(利用者ID)、302…利用者情報の読み込み(パスワード)、303…ICカードの読み取り、304…ICカードに登録済みデータがあるかどうかの判定、305…暗号化鍵Aの生成、306…利用者情報、暗号化鍵AのICカードへの書き込み、307…ICカードを初期化してよいかの判定、400…機密情報格納処理1開始、401…利用者情報の読み込み、402…ICカードの読み取り、403…利用者の入力が正しいかどうかの判定、404…機密情報の読み込み、405…ICカードからの暗号化鍵Aの読み込み、406…暗号化鍵Aによる暗号化処理、407…ハードディスクから暗号化鍵Bの取り出し、408…暗号化鍵Bによる暗号化処理、409…格納位置情報の利用者からの入力読み込み、410…格納位置情報のICカードへの書き込み、411…格納位置への暗号化された機密情報の格納、412…誤り回数カウンタへ1を足す処理、413…カウンタ回数判定、500…機密情報格納処理1開始、501…利用者情報の読み込み、502…ICカードの読み取り、503…利用者の入力が正しいかどうかの判定、504…ICカードから格納位置情報の読み込み、505…暗号化された機密情報の読み込み、506…ハードディスクから暗号化鍵Bの取り出し、507…暗号化鍵Bによる復号処理、508…複写先情報の利用者からの入力読み込み、509…暗号鍵Bで復号された機密情報(鍵Aで暗号化されている)の複写先への格納、510…誤り回数カウンタへ1を足す処理、511…カウンタ回数判定、600…機密情報格納処理1開始、601…利用者情報の読み込み、602…ICカードの読み取り、603…利用者の入力が正しいかどうかの判定、604…入力元情報の利用者からの入力読み込み、605…暗号鍵Bで復号された機密情報(鍵Aで暗号化されている)の入力元からの読み込み、606…ハードディスクからの暗号化鍵B'の取り出し、607…暗号化鍵B'による暗号化処理、608…格納位置情報の利用者からの入力読み込み、609…ICカードの格納位置情報の書き換え、610…格納位置への暗号化された機密情報の格納、611…誤り回数カウンタへ1を足す処理、612…カウンタ回数

40 判定。

【図1】

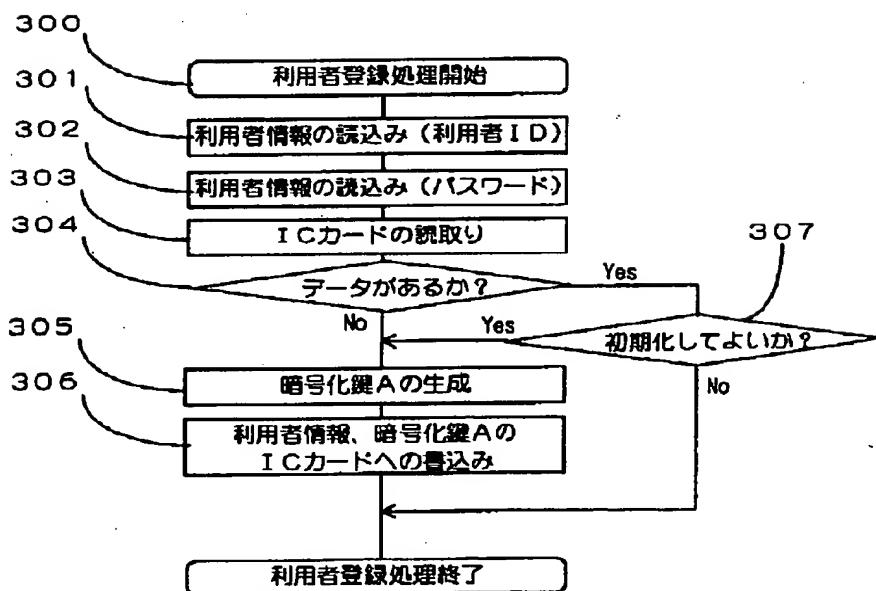


【図2】



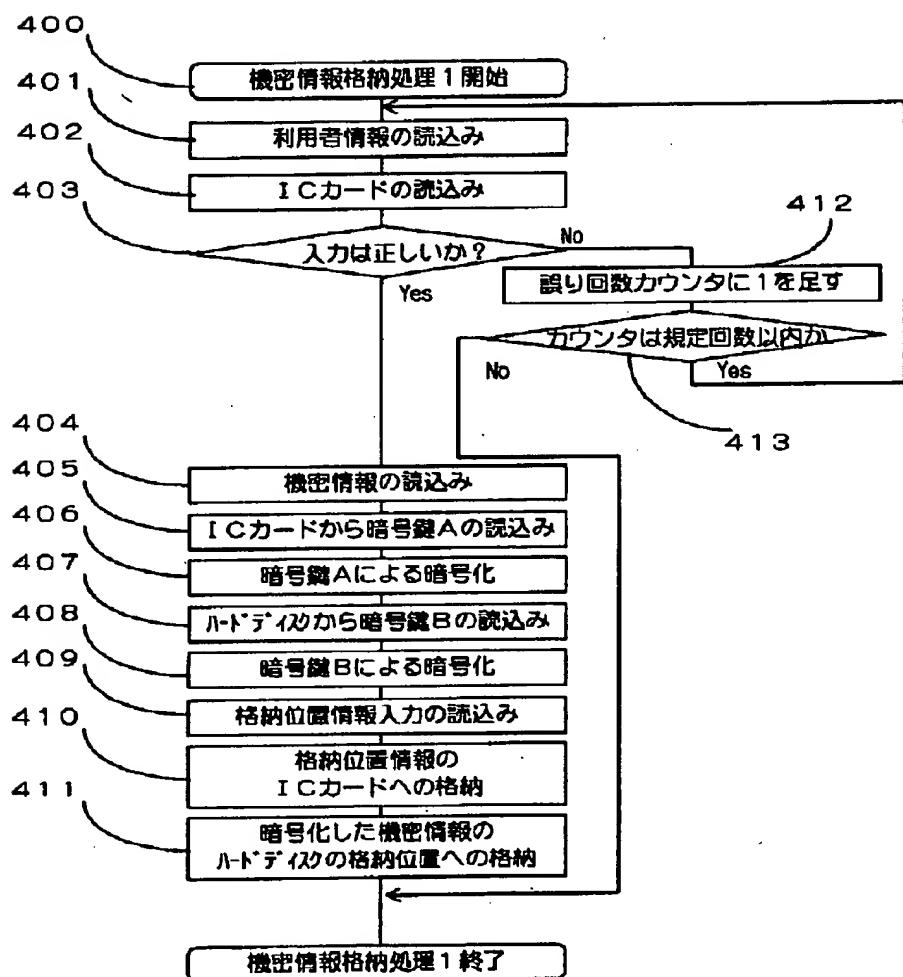
【図3】

図3



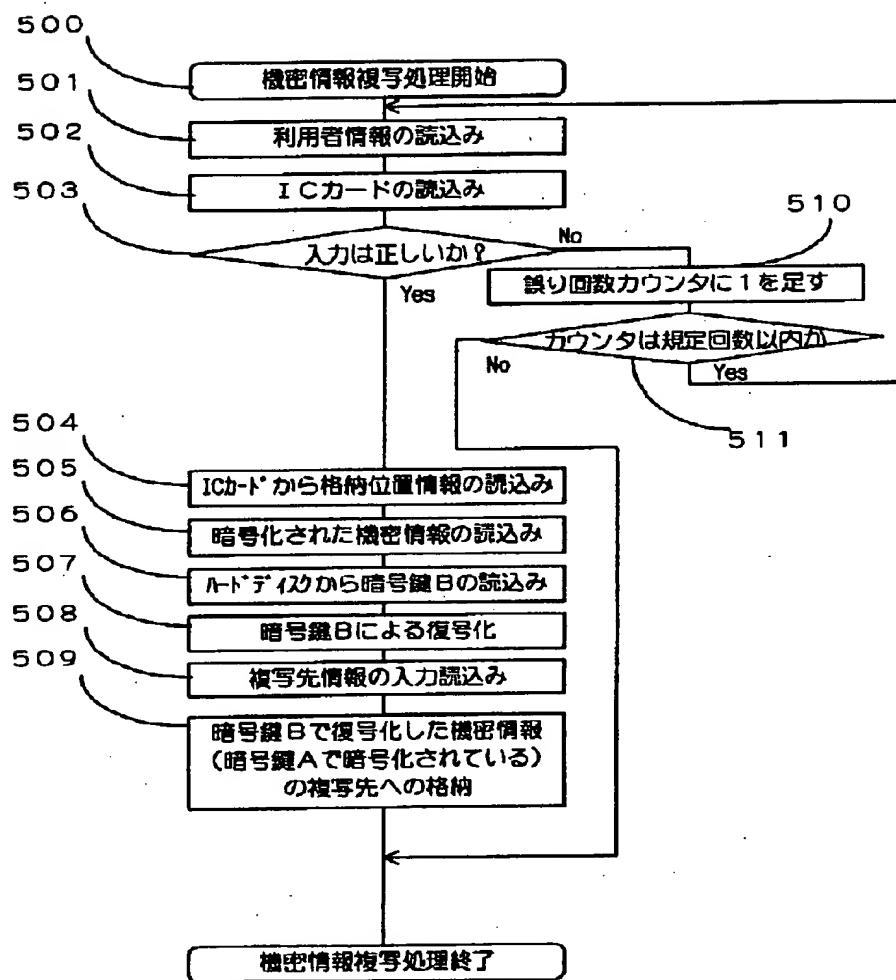
【図4】

図4



【図5】

図5



【図6】

図6

